

# CLAIMS

Sub  
B1

1. A method for synchronizing a stream cipher comprising:
  - 2 transmitting a control set of numbers indicating a current state of the stream cipher at a transmission source; and
  - 4 using the control set of numbers to determine the current state of the stream cipher at a reception site.
2. The method of Claim 1, wherein the control set of numbers comprises a cycle number.
3. The method of Claim 2, wherein the transmission source is a mobile station and the reception site is a base station.
4. The method of Claim 2 wherein the step of determining the current state of the stream cipher is accomplished by the formula:
 
$$S_{n+k} = C_{k-1}S_{n+k-1} + C_{k-2}S_{n+k-2} + \dots + C_1S_{n+1} + C_0S_n$$
 wherein  $k$  is the size of a linear shift register,  $n$  is the cycle number,  $s_i$  is an element stored in a linear shift register with  $n \leq i \leq n+k-1$ , and  $c_j$  is a constant with  $0 \leq j \leq k-1$ .
5. The method of Claim 4 wherein the step of determining the current state of the stream cipher at the base station is accomplished by:
  - using a first array of numbers and the cycle number to determine a second array of numbers; and
  - using the second array of numbers and a first set of numbers to determine the current state of the stream cipher at the base station.
6. The method of Claim 5, wherein the second array of numbers is determined by performing a series of multiplication operations of the first array of numbers with itself, wherein the number of multiplication operations is determined by the cycle number.

094344 "24E8E460

2

4

6

8

10

2

2

4

6

2

4

6

12. The method of Claim 11 wherein the second array of numbers is  
 2 determined by performing a series of multiplication operations of the first array  
 of numbers with itself, wherein the number of multiplication operations is  
 4 determined by the cycle number.

13. The method of Claim 11, wherein the second array of numbers is pre-  
 2 calculated and is stored by the first recipient before the step of transmitting the  
 control set of numbers.

14. The method of Claim 2, wherein the control set of numbers comprises a  
 2 stutter number.

15. The method of Claim 14, wherein the step of transmitting the control set  
 2 of numbers comprises the step of transmitting from a mobile station to a base  
 station.

16. The method of Claim 14 wherein the step of determining the current  
 2 state of the stream cipher is accomplished by the formula:

$$S_{n+k} = C_{k-1}S_{n+k-1} + C_{k-2}S_{n+k-2} + \dots + C_1S_{n+1} + C_0S_n$$

4 wherein  $k$  is the size of a linear shift register,  $n$  is the cycle number,  $s_i$  is  
 an element stored in a linear shift register with  $n \leq i \leq n+k-1$ , and  $c_j$  is a constant  
 6 with  $0 \leq j \leq k-1$ .

17. The method of Claim 16 wherein the step of determining the current  
 2 state of the stream cipher at the base station is accomplished by:

using a first array of numbers and the cycle number to determine a  
 4 second array of numbers; and

using the second array of numbers and a first set of numbers to  
 6 determine the current state of the stream cipher at the base station.

18. The method of Claim 17, wherein the second array of numbers is  
 2 determined by performing a series of multiplication operations of the first array

65T.T.T. "24E8E.H6D" P1

of numbers with itself, wherein the number of multiplication operations is determined by the cycle number.

19. The method of Claim 17, wherein the second array of numbers is pre-calculated and is stored by the first recipient before the step of transmitting the control set of numbers.

20. The method of Claim 14, wherein the step of transmitting the control set of numbers comprises:

transmitting an encrypted data stream from a first source to a plurality of recipients, wherein the encrypted data stream is encrypted using the stream cipher;

transmitting a plurality of cycle numbers from the first source to the plurality of recipients; and

determining a current state of the stream cipher by using the plurality of cycle numbers by each of the plurality of recipients, wherein each of the plurality of recipients uses one of the plurality of cycle numbers.

21. The method of Claim 20 wherein each of the plurality of recipients determines a different current state of the stream cipher.

22. The method of Claim 20 wherein the step of determining the current state of the stream cipher is accomplished by the formula:

$$S_{n+k} = C_{k-1}S_{n+k-1} + C_{k-2}S_{n+k-2} + \dots + C_1S_{n+1} + C_0S_n$$

wherein  $k$  is the size of a linear shift register,  $n$  is the cycle number,  $s_i$  is an element stored in a linear shift register with  $n \leq i \leq n+k-1$ , and  $c_j$  is a constant with  $0 \leq j \leq k-1$ .

23. The method of Claim 22 wherein the step of determining the current state of the stream cipher is accomplished by:

using a first array of numbers and a cycle number to determine a second array of numbers; and

094344-1-24E8E460

using the second array of numbers and a first set of numbers to  
6 determine the current state of the stream cipher.

24. The method of Claim 23, wherein the second array of numbers is  
2 determined by performing a series of multiplication operations of the first array  
of numbers with itself, wherein the number of multiplication operations is  
4 determined by the cycle number.

25. The method of Claim 23, wherein the second array of numbers is pre-  
calculated and is stored by the first recipient before the step of transmitting the  
control set of numbers.

26. An apparatus for synchronizing a stream cipher comprising:

2 means for determining a cycle number;

means for determining a stutter number;

4 means for transmitting the cycle number and the stutter number to a remote recipient; and

6 means for using the cycle number and the stutter number to determine the current state of the stream cipher, wherein said means for using the cycle

8 number and the stutter number is located at the remote recipient.